UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
BOSTON DIVISION

JAGEX LIMITED,	)	
	)	**Case No. 1:10-cv-10216**
PLAINTIFF,	)	
	)	
v.	)	
	)	
IMPULSE SOFTWARE, **ERIC SNELLMAN, and** **MARK SNELLMAN**	)	
	)	
DEFENDANTS.	)	
	)	

DEFENDANTS' MEMORANDUM IN RESPONSE TO PLAINTIFF'S MOTION FOR PROTECTIVE ORDER

Defendants, IMPULSE SOFTWARE, ERIC SNELLMAN and MARK SNELLMAN ("Defendants") by and through their undersigned attorneys, hereby file this Memorandum in Response to Plaintiff's, JAGEX LIMITED ("JAGEX" or "Plaintiff") Motion for a Protective Order and states:

Like Plaintiff, Defendants also seek entry of a protective order. Both parties possess respective source codes that are of a highly sensitive and confidential nature. However, Plaintiff's proposed protective order is designed to oppress and place an undue burden and expense on Defendants. Plaintiff's proposed protective order is oppressive and burdensome since it limits the authorized representatives of Defendants access to Plaintiff's source code to either Boston or the United Kingdom, even though the offices of Defendants' lead counsel are in Orlando, Florida. Plaintiff's proposed protective order is also delaying access to Plaintiff's source code for up to a week when access is requested. Defendants, on the other hand, seek a protective order that balances both parties' concerns as each party accesses the opposing party's highly sensitive and confidential information in preparing their respective cases.

The parties did conferred in an attempt to agree on a joint order. However, without any regard to the burden it would impose on Defendants, Plaintiff insisted on overreaching restraints. When Defendants asked Plaintiff for a legal basis to justify the restraints it sought to place upon Defendants, as contained in paragraph 27 of Plaintiff's proposed protective order, Plaintiff failed to do so. *See* Exhibit "A". Just as Plaintiff initially sought to unduly burden Defendants by only planning to make its witnesses available in the United Kingdom[1], Plaintiff is again taking an untenable position that greatly disadvantages Defendants. Plaintiff is taking this position even though the Court verbally stated to both parties, several times, at the Scheduling Conference on October 1, 2010 that the Court did not expect the parties to disagree over language in a stipulated protective order. The Court further explained to the parties that such disputes typically result in the prevailing party being awarded attorney's fees.

Plaintiff's position in its proposed protective order is also prohibiting production of written discovery. Though both parties have submitted a first set of written discovery, much of what should have been disclosed is not being disclosed because a protective order is not in force. This delay is hampering Defendants' efforts of submitting additional written discovery before the deadline to submit written discovery (December 31, 2010).

Defendants have attempted to provide a protective order that includes the security protections that Plaintiff seeks while not overly burdening Defendants. For these reasons, Plaintiff's proposed Protective Order should not be considered and Defendants' Protective Order, which balances both parties' interests, should be entered by the Court instead.

[1] The Court interceded with this issue by directing that Plaintiff pay for Defendants' attorneys to take depositions of Plaintiff's employees in the United Kingdom.

I. Use of a Protective Order as both a Sword and a Shield is Improper

Plaintiff's explanation about how it has maintained the confidentiality of its source code during the normal course of its business prior to suing Defendants is admirable, but is immaterial in this action. Plaintiff made a conscious decision to file suit against Defendants here in the United States. Two of the counts levied against Defendants are Copyright Infringement and Circumvention of Technological Measures under the Digital Millennium Copyright Act. [Dkt. No. 35] Thus, Plaintiff is using its source code as a sword in its attack upon Defendants, and yet should have known that the type of access sought by Defendants was expected. Because of Plaintiff's actions, Defendants' lead counsel and designated experts or consultants must have reasonable access to Plaintiff's source code to prepare a defense to defend against Plaintiff's claims. Presumably, Plaintiff's counsel will also require similar access to Defendant's source code.

As is typical in litigation, as facts become known, theories are developed, and legal arguments are refined. A party will likely require numerous opportunities to access information protected by a protective order, especially when the underlining basis of the complaint is information protected by the protective order. Such access should not be inordinately impeded.

Plaintiff's alleged copyright of its source code is not a United States registered copyright. Instead Plaintiff has alleged owning *at least one* unregistered copyright[2] in the source code under the copyright laws of the United Kingdom, the Berne Convention, and the United States. [Dkt. No. 35]. Plaintiff presumably makes this claim because the United Kingdom (hereinafter "the UK") does not have a copyright registration procedure, and even though it has registered other copyrights here in the United States, Jagex has made a strategic decision not to register its source

[2] Without a registration Defendants are without knowledge as to how many copyrights of its source code Plaintiff is claiming.

code in the United States. Thus, until Plaintiff provides access to its source code, Plaintiff's alleged copyrighted source code is not available anywhere.

As for its technological measures which it claims are being circumvented, Plaintiff has not identified any information about such measures, not even a name. *Cf. MDY Indus., LLC v. Blizzard Entm't, Inc.*, 2010 U.S. App. Lexis 25424 (9th Cir. December 14, 2010) (noting that Blizzard developed a technology known as "Warden" to prevent its players from using unauthorized third-party software including bots). Defendants continue to maintain that no unique programming is utilized in their source code to circumvent a technological measure in Plaintiff's source code. Defendants, through their lead counsel and qualified experts or consultants, will require access to Plaintiff's source code to ascertain if any technological measures are actually in place, and if there are any, whether or not Defendants' source code circumvents these measures.

Plaintiff seeks to impose a substantial financial burden on Defendants when Defendants' lead counsel and experts seek to examine Plaintiff's source code. In Paragraph 27(b) of their proposed Protective Order, Plaintiff seeks to only make its source code available at a Source Code review facility, located at the facilities of the Producing Party (for Plaintiff this would mean in the United Kingdom) or at the offices of the Producing Party's Outside Litigation Counsel within the District of this Court, at the Receiving Party's election. [Dkt. No. 43-2]. Such unjustified limitations practically, logistically, and financially limit the frequency that Defendants' lead counsel and Qualified Experts could have access to Plaintiff's source code since Defendants' lead counsel's offices are in Orlando, Florida.

Plaintiff further includes time-delaying requirements for Defendants to access Plaintiff's source code. In Paragraph 27(d), Defendants are required to provide Plaintiff at least one week's notice prior to any inspection of the source code to allow the Producing Party to coordinate administrative aspects of the source code inspection. If Plaintiff's counsel is maintaining the Jagex source code in a secure location on a stand-alone secure computer system(s), requiring at least one week's notice is nonsensical. Furthermore, if Defendants' lead counsel required access as they prepared for trial, after the discovery period ended, this inordinate time delay plus the time expended traveling to Plaintiff's facility and then returning to their Florida offices is extremely excessive.

As crafted and if accepted by the Court, Plaintiff would be allowed to wield its proposed protective order and it's source code as a sword against Defendants, and at the same time as a shield to impede Defendant's lead counsel from defending Defendants. Courts have found that such actions are improper. *See, e.g., Sony Computer Entm't Am., Inc. v. Nasa Elecs. Corp.*, 249 F.R.D. 378 (S.D. FL 2008) (concluding that a party should not be permitted to use a protective order as both a sword and a shield by resting their defenses on third parties and then restricting efforts of the opposing party to test their defenses by examining those third parties).

II. The Named Parties Will Not Have Access to the Opposing Party's Source Code.

Even though Plaintiff argues that the named Defendants should not have access to Plaintiff's source code, nowhere in either party's proposed protective order are any of the named parties granted access to the Producing Party's source code. Instead, terms are provided in both parties' proposed protective order prohibiting such access. *See* Dkt. 43-2 paragraphs 6 and 7 and Exhibit "B", paragraphs 6 and 7. Thus, Plaintiff's argument about the actual defendants having access is completely irrelevant.

Defendants submit that Plaintiff's position suggests that instead of recognizing that Defendants' lead counsel are officers of the Court, just as Plaintiff's counsel are such officers, Defendants' lead counsel should not be trusted. All attorneys in this case have equivalent legal and deontological obligations to ensure that confidentiality in the functioning of the judicial system as a whole, in order to forge justice out of the application of the law and the simultaneous pursuit of the legitimate interests of all parties and the general good of society is maintained. Defendants' lead counsels are in good standings with the Court and all other courts and governmental agencies in which they are admitted to practice law. Thus, allowing Defendants' lead counsel access to Plaintiff's source code at a location convenient to Defendants' lead counsel's offices (including at lead counsel's offices) is fair, just, and proper.

With respect to their own source code, Defendants believe that as officers of the Court, Plaintiff's attorneys will not use Defendants' software for a nefarious purpose, such as disclosing Defendants' source code to entities excluded by either party's proposed protective order. Instead, Defendants believe that Plaintiff's attorneys will abide by a protective order entered by the Court. Thus, under Defendants' proposed protective order, Defendants are comfortable with Plaintiff's attorneys having access to Defendants' software at their offices, whether in Boston or Washington, D.C.

III. The Model Stipulated Protective Order Provided by the Northern District of California Best Addresses the Issues Before the Court

Federal Rule of Civil Procedure 26(c)(1) provides that "the court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way." FED. R. CIV. P. 26(c)(1). Though source code may be recognized as confidential information, Plaintiff's overreaching mandates in its proposed protective order is to protect its source code by placing an undue burden and expense on Defendants. In substantiating its desire to unduly burden Defendants, Plaintiff cites to other examples of protective orders from other Federal District Courts, namely the Eastern District of Texas, the Northern District of California, and the District of Delaware. However each example actually is more supportive of Defendants.

With respect to the Northern District of California, Plaintiff utilized the Patent Local Rule 2-2 Interim Model Protective Order to substantiate its desired overreaching requirements in its proposed protective order. Yet, even though Plaintiff has emphasized the highly sensitive confidential nature of its source code, even equating it to a trade secret, Plaintiff did not identify to the Court the Northern District of California's Stipulated Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets to the Court, the Northern District of California (hereinafter "the California Stipulated Protective Order"). *See* Exhibit "C". The California Stipulated Protective Order is actually more appropriate considering the significance of the source code involved. The California Stipulated Protective Order articulates the following solution when the receiving party and producing party are in different jurisdictions:

> "Any source code produced in discovery shall be made available for inspection in a format through which it could be reasonably reviewed and searched during normal business hours or other mutually agreeable times at a location that is reasonably convenient for the Receiving Party and any experts to whom the source code may be disclosed. This alternative may be appropriate if the Producing Party and/or its counsel are located in a different jurisdiction than counsel and/or experts for the Receiving Party."

See Exhibit "C", fn. 15.

From the Eastern District of Texas, Plaintiff identifies a pending case, *Paltalk Holdings, Inc. v. Sony Computer Entm't Am., Inc., et al.*, No. 2:09-cv-00274 (hereinafter "the Texas case"), in which Jagex is a named defendant. However, in that case, Jagex is being sued for patent infringement. For reasons only known to the parties in that unrelated suit, all parties stipulated to each producing party only having to provide stand-alone secure computer system(s) at facilities of the Producing party or, at the Producing Party's election, the offices of the Producing Party's Outside Litigation Counsel.

The plaintiff in the Texas case likely does not have confidential material since its basis for suit is a patent. Defendants suspect that the plaintiff of the Texas case agreed to travel to each defendant's facilities or offices of its respective outside litigation counsel to evaluate each defendant's alleged infringing products to prove infringement of its patent so that the stipulated protective order could be acceptable to all parties. Thus, just as Jagex, a named defendant in the Texas case, was not unduly burdened, Defendants seek not to be unduly burden in the subject suit.

The facts in *Polycom, Inc. v Codian Ltd.*, 2007 WL 194588 (E.D. Tex. 2007) are also distinguishable. In *Polycom*, Plaintiff was provided a hard copy of the source code. Plaintiff sought a change to its access to the electronic source code even though its experts had already spent several months, at the defendant's facility, inspecting the electronic source code. As clearly articulated by Plaintiff in its memorandum, Defendant will not be provided a complete hard copy of the source code.

As for the Stipulated Protective Order in *Leader Technologies, Inv. v. Facebook, Inc.*, No. 1:08-cv-00862, this again is a protective order that was agreed upon between the parties. Furthermore, lead counsel for the opposing parties resided in Wilmington, Delaware and the attorneys admitted *Pro Hac Vice* for the opposing parties were from the Silicon Valley area of Northern California. *See* Composite Exhibit No. "D" (Docket report and other documents illustrating locations of attorneys involved in *Leader Technologies*).

IV. Defendants' Proposed Protective Order Should be Entered

Exhibits "B" and "E" are Defendants' proposed protective order. For the Court's convenience, Exhibit "E" includes track changes annotations so that the Court can follow the changes between the two proposed protective orders. Exhibit "B" is a clean version of Defendant's proposed protective order without the track changes annotations. Defendants' proposed order provides for a more equitable protective order.

Pursuant to the California Stipulated Protective Order, Defendants seek to have the Producing Party provide their source code on up to two independent stand-alone secure computer system(s) at a location that is reasonably convenient to the offices of the lead counsel of the Receiving Party's Outside Litigation Counsel, at the request of and use by the Receiving Party. *See* Ex. "B", Paragraph 27(b) and Ex. "E", Paragraph 27(b). This location may be lead counsel's offices or another location convenient to lead counsel's offices.

Defendants further seek to reduce the built in time-delay that the Plaintiff is requesting when before the Receiving Party can obtain access the source code, or receive printouts of the hard copies of the source code. In Paragraph 27(d) as amended, Defendants believe that a four (4) hour advance notice requirement is sufficient enough when the stand-alone secure computer system(s) are provided at a location reasonably convenient to the offices of the lead counsel of the Receiving Party's Outside Litigation Counsel, but when the location is not the lead counsel's offices. *See* Ex. "B", Paragraph 27(d) and Ex. "E", Paragraph 27(d). Since the Receiving Party cannot print copies of any segments of the source code, Defendants seek to limit the delay of providing copies requested from four (4) days to two (2) days. *See* Ex. "B", Paragraph 27(h) and Ex. "E", Paragraph 27(h).

In Paragraph 27(c) Defendants have removed the last sentence since it appears to conflict with the second sentence of this paragraph. *See* Ex. "B", Paragraph 27(c) and Ex. "E", Paragraph 27(c).

Under Plaintiff's proposed protective order, the only entity with control over the Producing Party's source code is the Producing Party. A copy of the Producing Party's source code could be altered or revised without the Receiving Party ever knowing. Defendants have included a clause, Paragraph 27(m), to provide for an approach to allow the Receiving Party to determine whether the source code initially provided by the Producing Party is the same source code throughout the course of litigation. *See* Ex. "B", Paragraph 27(m) and Ex. "E", Paragraph 27(m).

In Paragraph 24, an additional clause has been added to address the return of the stand-alone secure computer system(s) to the Producing Party at the conclusion of this litigation if the Producing Party provides these computer system(s) at the offices of the lead counsel of the Receiving Party's Outside Litigation Counsel. *See* Ex. "B", Paragraph 24 and Ex. "E", Paragraph 24.

In Paragraph 7, Defendants have removed the requirement of returning the Representative Sample within ten (10) days since this requirement is vague. Both proposed orders already provide provisions for handling hard copies of source code, so a requirement to return the Representative Sample after 10 days is an exceptional requirement. Furthermore, if Defendants opt to interview more than one prospective qualified expert, it is unclear when this 10 day window begins. Finally, under U.S. Copyright laws, deposit of the source code, or at least a certain number of pages of the source code, must be deposited with the Copyright Office. Such a deposit is available to the public for inspection. Defendants consider the Representative Sample equivalent to the deposit required in the United States. *See* Exhibit "F" (Circular 61 from the United States Copyright Office).

There are other overreaching requirements that Defendants are concerned about and would prefer to address now, but out of respect for Plaintiff's heightened security concerns, Defendants have decided to wait until their qualified expert is available to further determine what type of access may be needed to provide a proper defense. For example, Defendants may have to compare Plaintiff's source code next to, or interacting with, Defendants' source code, such as by utilizing an electronic diagnostic device that will map functions of both source codes as they operate to determine if a technical measure is being circumvented. As both parties' protective orders are currently written, this is not possible since the computers holding the source codes are stand-alone secure computer systems which may not interact with such a device or system. Going forward, Defendants will again attempt to work in good faith with Plaintiff if such further access beyond what is provided in either proposed protective order is required, hopefully with a result that will not require the Court's intervention.

WHEREFORE, so as not to oppress, or undue burden or expense either party, while balancing the security interest of both parties, Defendants respectfully request that this Court enter the attached Protective Order provided as Exhibit "B" to this memorandum, and if the Court deems it appropriate, an award of Defendants attorneys' fees for having to prepare this Response.

Dated this 17th day of December, 2010.

Respectfully submitted,

IMPULSE SOFTWARE, et al
By its attorneys,

/s/ Terry M. Sanks
BEUSSE WOLTER SANKS MORA & MAIRE, P.A.
Terry M. Sanks (Florida Bar No. 0154430)
Amber Davis (Florida Bar No. 0026628)
390 North Orange Avenue, Suite 2500
Orlando, Florida 32801
Telephone: (407) 926-7700
Facsimile: (407) 926-7720
tsanks@iplawfl.com
adavis@iplawfl.com
Lead Counsel to Defendants

-And-

HOLLAND & KNIGHT LLP
Ieuan G. Mahony (BBO #552349)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700
ieuan.mahony@hklaw.com
Local Counsel to Defendants

CERTIFICATE OF SERVICE

I Hereby Certify that a true and correct copy of the foregoing was filed with the Court on the 17th day of December, 2010 by utilizing the CM ECF System which will serve via E-mail a copy of the foregoing upon the following interested parties: Christopher Roth, Esquire, (croth@bannerwitcoff.com); Peter McDermott, Esquire, (pmcdermott@bannerwitcoff.com); Ross Alan Dannenberg, Esquire, (rdannenberg@bannerwitcoff.com); and Erin E. Bryan, (ebryan@bannerwitcoff.com); Banner & Witcoff, Ltd., 1100 13th Street, N.W., Suite 1200, Washington, D.C., 20005-4051.

/s/ Terry M. Sanks
Attorney